Introduction to Physical Security

Student Guide

September 2017

Center for Development of Security Excellence

Lesson 1: Course Introduction

Introduction

Welcome

Every day, on our military installations and within DoD facilities, we protect a wide variety of assets from various types of threats. One way we do this is through the use of physical security to deter and detect intruders. Welcome to the Introduction to Physical Security course. In this course, you will learn about physical security concepts and roles, as well as physical security planning and implementation, including a review of the various types of physical security countermeasures employed to deter, delay, detect, or prevent threats.

Objectives

Here are the course objectives:

- Identify the terms, concepts, and policies associated with physical security
- Identify and define the roles and responsibilities of personnel in the physical security program
- Identify physical security countermeasures and their uses in the protection of DoD assets
- Describe physical security planning, antiterrorism, force protection and their tools

Lesson 2: Physical Security Overview

Introduction

Objectives

In this lesson, we'll explore what physical security, security-in-depth, and the risk management process are. We'll also review the policies that outline the requirements for physical security.

Here are the lesson objectives:

- Identify the purpose of physical security
- Define security-in-depth
- Identify the purpose and steps of the risk management process
- Identify the policies that outline the requirements for physical security

What Is Physical Security?

Purpose

A major responsibility for installations and facilities, the purpose of physical security is prevention and protection. Physical security is defined as that part of security concerned with active, as well as passive measures, designed to deter intruders, prevent unauthorized access, including theft and damage, to assets such as personnel, equipment, installations, materials, and information, and to safeguard these assets against threats such as espionage, sabotage, terrorism, damage, and criminal activity.

Security-in-Depth

The protection of national security and other DoD assets is accomplished through the application of active and passive complementary security controls. This integration of physical security measures is also known as security-in-depth. Security-in-depth is a determination by the senior agency official that a facility's security program consists of layered and complementary security controls sufficient to deter, detect, and document unauthorized entry and movement within the facility. This is accomplished through the integration of active and passive complementary physical security measures.

The best way to describe how security-in-depth works is to think of an onion and all the layers it takes to get through to the center. As you begin to peel an onion, it takes more of an effort to reach the center.

Let's take a government facility and add barriers and guard posts with guards in them. Next, add a fence around the perimeter along with bright lights and appropriate signs. The government building inside the fence also employs security measures, as there will be guards and security screening equipment one must walk through to get into the building.

Can you see the layers of security and how each one is a deterrent? If someone is able to penetrate any one of these layers of security, it will take them time and energy to get through to the next layer. That time is what enables our security to defend and protect our national security and DoD assets.

Security requirements for classified contracts are stated in Department of Defense (DoD) 5220.22M, the National Industrial Security Program Operating Manual (NISPOM). Any additional security requirements levied upon a contractor must be specifically addressed in the contract.

Point vs. Area Security

Two applications of physical security are point security and area security.

Point security is exactly how it sounds. If you are assigned to point security, you are guarding a specific asset or resource. A good example of point security is the original Constitution of the United States of America. There are guards standing directly in the space of the constitution. On our military installations or secure federal buildings, entry, and exit locations are often guarded. This is also an example of point security. Now that you know what point security means, what do you think area security might mean?

Area security protects an entire area of the installation or facility. The goal of area security is to try and consolidate as many assets as possible into one area. This is to intensify the protection efforts while maximizing the effectiveness of response forces. It is important to remember that security professionals employ both point and area security to protect national security and other DoD assets from damage, loss, and theft.

Risk Management Process

In order to plan and implement effective physical security measures, you must use the risk management process to determine where and how to allocate your security resources. The steps in the risk management process are:

- Identify assets
- Identify threats
- Identify vulnerabilities
- Conduct risk analysis
- Determine countermeasure options
- Make risk management decisions

Let's take a look at each step in the risk management process to learn more.

Identify Assets

Properly designed and executed physical security programs should deter or prevent, to the greatest degree possible, the loss of, theft of, or damage to an asset. DoD assets include people, information, equipment, facilities, activities, and operations. Combined, these assets are referred to as PIE-FAO. When identifying and assessing an asset, you must determine the nature and value of that asset and the degree of impact if the asset is damaged or lost.

Identify Threats

After identifying assets you must identify and assess the threats to those assets. A threat is the perceived imminence of intended aggression by a capable entity to harm a nation, a government, or its instrumentalities, such as intelligence, programs, operations, people, installations, or facilities. A threat can be an indication, circumstance, or event with the potential to cause loss of, or damage to, an asset or capability. Examples of threats include threats from the Foreign Intelligence agents, terrorist organizations, foreign military or paramilitary forces, criminal activities, civil disturbances, insider threats, environmental threats, and cyber threats.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Threat: The perceived imminence of intended aggression by a capable entity to harm a nation, a government, or its instrumentalities

Foreign Intelligence Agents: Adversaries acting in the interest of a foreign intelligence entity that actively engages in intelligence activities against the U.S. or its assets

Terrorists/Saboteurs: Adversaries who use violence or the threat of violence to instill fear with the intent to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological

Foreign Military/Paramilitary Forces: Terrorist groups develop organizational structures that are functional for the environment in which they operate, such as cellular and paramilitary. Terrorist organizations are military in nature, with a set chain of command. There are four elements in this structure: leaders, active cadre, active supporters, and passive supporters.

Criminals: Adversaries who commit crimes against people or property such as assault, theft, or hacking into computer systems

Civil Disturbances: Civil disturbances most often arise from political grievances, urban economic conflicts, community unrest, terrorist acts, or foreign influences. They can range from peaceful picketing to full-blown riot situations.

Insider Threats: Trusted persons who have been granted access to DoD resources or services Environmental Threats: Natural phenomena/disasters that have the potential to damage DoD resources or services or interrupt activities or operations Cyber Threats: Attacks on DoD computer systems and the information contained in those systems.

Identify Vulnerabilities

After you have identified the assets and threats, you must identify the vulnerabilities and determine their extent.

Vulnerabilities are weaknesses, characteristics, or circumstances that can be exploited by an adversary to gain access to or information from an asset. If not addressed, vulnerabilities may result in the degradation, loss of life, or damage to mission-essential resources. Vulnerabilities can be the result of a variety of factors, such as the way a building was constructed, location of people and equipment, operational practices, and even personal behavior.

NOTE: The information in the box below will not be on the test but is included here as additional information that may provide useful background and insight.

Vulnerabilities: Situations or circumstances that, if left unchanged, may result in the degradation, loss of life, or damage to mission-essential resources

Conduct Risk Analysis

Once you have identified the assets, threats, and vulnerabilities, you must then conduct a risk analysis based on both the impact of an unwanted event and the likelihood that it could happen. Think about the impact if your assets were compromised and the likelihood of a compromise happening, such as loss of strategic or military advantage, or even loss of life.

Determine Countermeasure Options

Once you've calculated the risks, you must determine which countermeasures you might employ to protect DoD assets by reducing vulnerabilities and mitigating threats. Countermeasures include security measures that you employ in up-front facility design, in the day-to-day protection of DoD assets, and in times when threat levels increase.

Make Risk Management Decisions

Once you've determined your countermeasure options, you must make risk management decisions based on the cost versus the benefit of protecting DoD assets.

Policy Guidance

Executive Orders

Physical security has been around since the beginning of mankind. There has always been a need for the protection of one's belongings. Through the years, the purpose of physical security has largely remained the same: to protect our assets. However, the methods used in the DoD Physical Security Program have changed significantly.

In 1952, President Truman signed Executive Order 10421, which provided physical security for facilities deemed important to the national defense mission.

In 1962, President Kennedy signed Executive Order 11051, which made agency directors responsible for informing the President of actions necessary to physically protect facilities and other assets to national security.

In 1979, President Carter signed Executive Order 12148, which established the Federal Emergency Management Agency (FEMA) which is charged with planning for national emergencies.

In 1988, President Reagan signed Executive Order 12656, which established sufficient capabilities at all levels of government to meet essential defense and civilian needs during any national security emergency.

On June 25, 1996, the attack on U.S. forces housed in the Khobar Towers complex in Saudi Arabia changed attitudes on the protection of U.S. personnel from terrorist attacks. As a result of the Downing Commission Report, the Secretary of Defense accepted responsibility for anti-terrorism/force protection (AT/FP) efforts within DoD and designated the Chairman, Joint Chiefs of Staff (CJCS) as the focal point for all of DoD.

On September 11, 2001, the largest attack by terrorists in the U.S. occurred. As a result, the U.S. Congress passed, and President George W. Bush signed, the Homeland Security Act of 2002, which created the Department of Homeland Security (DHS). This represented the largest restructuring of U.S. government in contemporary history.

In October 2001, President Bush signed Executive Order 13228, which established the Office of Homeland Security and the Homeland Security Council, which coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States.

In October 2001, President Bush also signed Executive Order 13231, which ensures the physical security of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems.

In 2004, President Bush signed Homeland Security Presidential Directive (HSPD) 12 which mandated government-wide development and implementation of a standard for secure and reliable forms of identification for Federal employees and contractors.

In 2013, President Barack Obama signed Executive Order 13636 and Presidential Policy Directive (PPD) 21. Both of these directives strengthen the security and resilience of critical infrastructure against evolving threats and hazards while also incorporating strong privacy and civil liberties protections into every cybersecurity initiative. This Executive Order also calls for an updated and overarching national framework that reflects the increasing role of cybersecurity in securing physical assets.

DoD and Other Policy Guidance

There are several Department of Defense documents that govern physical security.

First DoD Instruction (DoDI) 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB) authorizes commanders to issue regulations for the protection or security of property and places under their command. This instruction also establishes guidelines to build consistent minimum standards for protecting DoD installations and resources.

DoD 5200.08-R, the Physical Security Program regulation, implements DoD policies and minimum standards for the physical protection of DoD personnel, installations, operations, and related resources.

DoDM 5200.01, the DoD Information Security Program manual, addresses the physical security aspects of protecting classified information within the information security program.

There are many other special categories that require physical protection not included in this training. If you are involved in such programs, consult the appropriate guidance. DoD security is governed by many programs. As a security professional, there may be times that you will need to refer to one of these documents for guidance. You do not need to recall the names and numbers of each of these documents. However, you should be aware of what information is available to guide you in the matters of physical security.

Review Activities

Review Activity 1

Question 1 of 3. The two primary purposes of physical security are protection and _______________?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Security-in-depth
- ○ Prevention
- ○ Point security
- ○ Area security

Question 2 of 3. A guard checking IDs at the gate of an installation is a good example of what type of security?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Security-in-depth
- ○ Prevention
- ○ Point security
- ○ Area security

Question 3 of 3. ___________ is the layering of physical security countermeasures such as fencing, guards, cameras, lighting, and locks.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Security-in-depth
- ○ Prevention
- ○ Point security
- ○ Area security

Review Activity 2

Before you can conduct a risk analysis based on the impact and likelihood of an unwanted event happening, what steps in the risk management process must you take first?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ Identify assets
- ☐ Identify threats
- ☐ Determine countermeasure options
- ☐ Identify vulnerabilities
- ☐ Make risk management decisions

Review Activity 3

Question 1 of 3. Which policy guidance would you consult to find the minimum standards for the physical protection of DoD assets?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ DoD 5200.08-R, Physical Security Program
- ○ DoDI 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)
- ○ DoDM 5200.01, Volumes 1-4 DoD Information Security Program

Question 2 of 3. Which policy should you consult to find the physical security requirements of protecting classified information?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ DoD 5200.08-R, Physical Security Program
- ○ DoDI 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)
- ○ DoDM 5200.01, Volumes 1-4 DoD Information Security Program

Question 3 of 3. Which policy authorizes commanders to issue regulations for the protection or security of property and places under their command?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ DoD 5200.08-R, Physical Security Program
- ○ DoDI 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)
- ○ DoDM 5200.01, Volumes 1-4 DoD Information Security Program

Lesson 3: Physical Security Roles and Responsibilities

Introduction

Objectives

In this lesson, we'll explore the roles of the individuals and coordinating activities charged with implementing physical security.

Here are the lesson objectives:

- Identify the individual physical security roles in the DoD and their responsibilities
- Identify the DoD working groups and committees who are charged with protecting our national security and other DoD assets

Individual Roles

Overview

The agencies and organizations that protect our national security and DoD assets are comprised of individuals who play an important part in the mission of physical security.

These individuals include the:

- Installation Commander or Facility Director
- Antiterrorism Officer (ATO)
- Counterintelligence (CI) support personnel
- Local, state and federal law enforcement officials
- Operations Security (OPSEC) Officer
- Physical Security Officer

Take a look at each role to learn more.

Installation Commander/Facility Director

Installation Commanders or Facility Directors who serve in management or leadership positions are responsible for several aspects of physical security. These responsibilities include the safety and protection of the people and property under their command, the planning, coordinating, and integrating of all physical security matters into their installation, and the identification of mission essential capabilities. DoDI 5200.08 designates commanders to issue regulations for the protection and security of property

or places under their command. In addition, the instruction authorizes the commander to take reasonably necessary and lawful measures to maintain law and order and to protect installation personnel and property.

Antiterrorism Officer

The Antiterrorism Officer manages the installation or facility antiterrorism program. This program uses defensive measures to reduce the vulnerability of individuals and property from terrorist attacks.

CI Support Personnel

CI support personnel are responsible for providing information on the capabilities, intentions, and threats of our adversaries. They must pay particularly close attention to those adversaries associated with foreign intelligence entities. History has proven that we must always be vigilant. In addition, CI support personnel are there to provide valuable assessments of counterintelligence considerations in support of physical security programs.

Law Enforcement Officials

Law enforcement officials are responsible for effective liaison with local, state, and federal law enforcement officials. This is vital in fostering good working relationships to coordinate support for antiterrorism concerns and efforts, and emergency response, as well as to address criminal incidents. Coordination activities support mutual understanding of jurisdiction and authority.

Operations Security Officer

The OPSEC Officer facilitates the process for identifying critical information, identifying threats to specific assets, assessing vulnerabilities to assets, analyzing risk to specific assets and to national security as a whole, and developing countermeasures against potential threats to national security and other DoD assets.

Physical Security Officer

The Physical Security Officer is charged with managing, implementing, and directing physical security programs. This person may also be responsible for the development and maintenance of physical security plans, instructions, regulations, and standard policies and procedures. They may also coordinate with local law enforcement agencies, antiterrorism officers, and loss prevention personnel.

Coordinating Activities

Overview

It is important for you to be familiar with the various coordinating activities that play a part in the physical security of DoD assets. These groups include the:

- Antiterrorism Executive Committee (ATEC)
- Antiterrorism Working Group (ATWG)
- Threat Working Group (TWG)
- Mission Assurance Senior Steering Group (MA SSG)

Physical security is not about one entity taking care of everything, but rather several coordinating activities providing an integrated and coherent effort for the protection of national security and other DoD assets.

Take a look at each coordinating activity to see the roles, responsibilities, and relationships between these groups.

ATEC

The Antiterrorism Executive Committee (ATEC) is an executive-level forum that meets at least semi-annually to develop and refine antiterrorism program guidance, policy, and standards and act upon recommendations of the Antiterrorism Working Group and Threat Working Group to determine resource allocation priorities and mitigate or eliminate terrorism-related vulnerabilities. When necessary, the ATEC integrates and aligns antiterrorism and mission assurance efforts, as the Mission Assurance Senior Steering Group does.

ATWG

ATWG stands for Antiterrorism Working Group. This group is responsible for assessing requirements for physical security, recommending and developing policy, preparing planning documents, and conducting criticality, vulnerability, and risk assessments. Members in the ATWG include the Antiterrorism Officer and representatives from all appropriate commands, organizations and tenant activities.

TWG

TWG is also known as the Threat Working Group. This group is responsible for identifying foreign, domestic, and local threats and informing the installation commanding officer (CO) of current threat trends in the area of responsibility.

The TWG is comprised of the Antiterrorism Officer, counterintelligence representative, law enforcement representative, operations security officer, information operations representative, and a chemical, biological, radiological, nuclear, and high yield

explosives (CBRNE) representative. Commanders of larger installations may choose to include more individuals in their TWG.

MA SSG

The Mission Assurance Senior Steering Group (MA SSG) meets quarterly to provide advocacy, coordination, and oversight to assist in both vertical and horizontal mission assurance alignment efforts on issues that cut across all DoD protection programs, including antiterrorism. This group functions as an Office of Secretary of Defense (OSD) and Joint Staff-level management and decision support forum with members of the Senior Executive Service and general or flag officers at the 1 and 2-star levels. Commanders of military installations and DoD facilities will ensure their ATEC communicates appropriate AT concerns through their Component chain of command or supervision to the MA SSG.

Review Activities

Review Activity 1

Question 1 of 3. Who is charged with management, implementation, and direction of all physical security programs?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Law Enforcement
- ○ Antiterrorism Officer
- ○ OPSEC Officer
- ○ CI Support
- ○ Physical Security Officer

Question 2 of 3. Who is responsible for providing valuable information on the capabilities, intentions, and threats of adversaries?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Law Enforcement
- ○ Antiterrorism Officer
- ○ OPSEC Officer
- ○ CI Support
- ○ Physical Security Officer

Question 3 of 3. Who is responsible for developing countermeasures against potential threats to national security and other DoD assets?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Law Enforcement
- ○ Antiterrorism Officer
- ○ OPSEC Officer
- ○ CI Support
- ○ Physical Security Officer

Review Activity 2

Which of the following individuals should be included in a Threat Working Group?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

- ☐ Antiterrorism Officer
- ☐ Counterintelligence (CI) representative
- ☐ Law enforcement representative
- ☐ Operations security officer
- ☐ Information operations representative
- ☐ Chemical, biological, radiological, nuclear and high yield explosive representative

Lesson 4: Physical Security Countermeasures

Introduction

Objective

In this lesson, we'll explore various physical security countermeasures used to protect DoD assets.

Here is the lesson objective:

- Identify physical security countermeasures and determine their uses in the protection of DoD assets

Site Design Considerations

Overview

Considerable thought goes into designing a secure facility, so it is protected from every angle. The way the site is designed is essential to the protection of mission capabilities, and is necessary for an effective physical security program. Properly designed facilities provide a physical and psychological deterrence to intruders. Poor facility design can also make a facility a possible target for intruders.

Take a look at a brief description of different security features.

- Warning signs can be easily read by persons approaching on foot or in a vehicle. Restricted area perimeter boundaries should be posted in conspicuous and appropriate places to clearly identify the area.
- Barriers and fencing are integral parts of all physical security systems. They establish boundaries and deter individuals.
- Natural defenses such as waterways, forestations, and ditches, or manmade obstacles such as barricades and vehicle barriers provide for difficult approaches or exit routes.
- Interior barriers establish boundaries or lines of demarcation of different activities within an installation.
- Protective lighting should enable guard force personnel to observe activities around or inside an installation without disclosing their presence. Adequate lighting discourages unauthorized personnel from entering a facility.

- Properly trained military working dogs supplement and enhance the capabilities of security forces and, therefore, facility protection.

Restricted Areas

Restricted areas are areas that require additional protection. Access is limited to authorized personnel. Restricted areas are designated for the security or safeguarding of property or material. Facility directors or installation commanders designate restricted areas. Restricted areas improve security by controlling access and providing additional layers of security. Warning signs displaying “Restricted Area” must be posted at the boundary of each restricted area so they can be easily read by persons approaching on foot or in a vehicle.

Building Protective Measures

When you look closely at all the elements it takes to construct a building, it is easy to see how there could be many vulnerabilities that could allow someone to enter and possibly access information that could damage our national security or other DoD assets. Protective measures inside and outside a building all play a role. Here are some examples of vulnerabilities, as well as protective measures than can be taken to make them more attack-resistant.

The number of entrances and exits should always be limited to the minimum necessary for mission accomplishment, as well as for emergency evacuation. Doors are considered a weak spot in a building. They are generally weaker than the building structure, making them less attack-resistant.

As a protective measure, doors can be made of solid steel.

Windows are also a significant weak point in a building, and are a huge vulnerability. As a protective measure, they can be covered with a protective film to make them shatter-proof.

Many roofs of buildings house air conditioners and ventilation systems. They, too, can easily be exploited if additional measures have not been taken to secure them.

Also, vents can be secured with steel bars. Based on the specific level, value, or sensitivity of information or equipment being protected in a facility, the requirements for construction may be different.

Types of Countermeasures

Overview

As you know by now, physical security covers many aspects of security around an installation or facility. Various types of physical security countermeasures include:

- Protective barriers
- Site lighting
- Security forces
- Security systems
- Facility access control
- Lock and key systems
- Storage containers and facilities

Let's take a closer look at each of these types of countermeasures.

Protective Barriers

The first line of defense in any physical security system is usually some form of perimeter protection system. The perimeter of an installation or facility is the outermost area of responsibility. Barriers and fencing are an integral part of this protection.

Fencing and barrier devices may be composed of several types of material. Fencing may be chain link, barbed wire, or concertina wire, to name a few. Other types of barriers may be poured concrete, hardened steel, or natural barriers.

Barriers are used for establishing boundaries, as well as deterring individuals from attempting unlawful or unauthorized entry. They can also be used as platforms for sensors such as lighting. And sometimes barriers can be used to prevent outsiders from viewing what occurs inside the perimeter. After the terrorist attacks on 9/11, you may have noticed that many barriers suddenly appeared in front of state and federal buildings. These barriers may have taken up some parking spaces or forced you to walk a longer distance to or from a building. However, as you can now see, they were put in place for a reason...to protect personnel and assets of the United States of America from potential terror attacks.

Site Lighting

Imagine for a moment that you are an intruder attempting to gain access to a military installation in order to photograph the stealth bomber. You have made it past the guard and the entrance, and over the cement barrier. You are sure you are home free because you just climbed down the barbed wire and have only one more obstacle between you and the stealth bomber. Suddenly, you hear a dog bark and simultaneously you hear a loud click, as a very bright piercing light is glaring in your face. You have no place to run, not only because you cannot see, but also because you have been caught by security forces. As you can see, there are layers of physical security in place for a reason. Site lighting is one of those layers.

Lighting can be used for several purposes. It enables guard force personnel to observe activities inside or around an installation. Adequate lighting for all approaches to an area not

only discourages attempted unauthorized entry, but also reveals persons within a given area. Lighting should supplement other protective measures such as fixed security posts or patrols, fences, and even alarms.

There are several varieties of lighting used by DoD installations and facilities including continuous, standby, emergency, and movable lighting. Continuous lighting is the most common protective lighting system. It consists of a series of fixed lights arranged to flood an area continuously with overlapping cones of light. Standby lighting is similar to continuous lighting, except the lamps are not continuously lit. They are used when additional lighting is necessary. Emergency lighting depends on alternative power sources and is therefore reserved for times when regular lighting is not available. Movable lighting is used when supplemental lighting is necessary.

Site lighting plays a large part in physical security and countermeasures to protect national security and other DoD assets. For more information on site lighting, refer to the Exterior Security Lighting eLearning course offered by the Center for Development of Security Excellence (CDSE).

Security Forces

Security forces are made up of DoD civilian personnel, military personnel, and contract personnel who are employees of a private or commercial source contracted by the federal government, and even trained dogs, all of whom play an active part in protecting our national security and other DoD assets. The majority of installations and facilities maintain a specially identified group of personnel who serve as the enforcement medium for the physical security program.

Typically, the security force protects areas such as static observation posts, which guard a high priority resource, and access control points that control access to a facility or secure area. They also serve as roving patrols who ensure the safety and security of the installation or facility to include personnel, information, equipment, and other DoD assets; response forces that respond to the alarms and incidents; security systems monitors who observe alarms and closed circuit television systems; dispatchers in control centers that dispatch response forces and mobile patrols and coordinate activities with other personnel; and escorts who are trained personnel responsible for pass and identification, and monitoring individuals.

Military Working Dogs

Military working dogs, also known as MWD or K-9s, are an integral part of the physical security program. Military working dogs are capable of performing many duties during law enforcement activities as directed by their handlers. These duties include seek, detect, bite and hold, and guard a suspect.

Military working dogs allow security force members to enforce laws and regulations, and protect DoD installations, facilities, and resources. These dogs can deter attack and defend their handlers during threatening situations. Military working dogs can assist in crowd control and confrontation management, as well as search for subjects, both indoors and outdoors. Certain working dogs are specially trained to detect drugs, which makes them a valuable asset to installation commanders.

Working dogs are also exceptionally valuable in antiterrorism operations. They can detect unexploded ordnance and search bomb threat scenes. In war fighting roles, military working dog teams provide enhanced patrol and detection capability to perimeter and point defense. Man's best friend is one of our nation's most valuable assets in our physical security mission.

Security Systems

Security systems play an important role in protecting national security and other DoD assets. Security systems include:

- Interior intrusion detection systems (IDS)
- Exterior IDS
- Closed circuit television (CCTV) systems
- Access control systems
- Screening equipment
- Two-way radios

Take a closer look at each type of security system to learn more.

Interior IDS

An intrusion detection system (IDS) is an important part of physical security. The purpose of an IDS is to deter, detect, document, and deny or delay intrusion. Intrusion detection systems detect changes in the environment which could be a result of an intruder, or something else that may require further investigation.

There are four types of interior IDS. Volumetric detectors are designed to detect a change in the environment in a particular area. There are both active and passive volumetric detectors. Operable opening switches are used on doors, windows, and other similar openings. They work with a magnetic switch, balanced magnetic switch (BMS) or high security switch (HSS). The BMS and HSS should be used in areas requiring high security. Interior barrier protectors are used to protect against amateur intruders. These include an infrared beam or a trip wire. Proximity detectors provide point security, and are used to protect items inside a building. They are composed of a capacitance detector and a pressure mat.

Exterior IDS

There are several types of exterior sensors in use throughout DoD.

Fence disturbance sensors do just what their name implies. They detect disturbances of the fence.

Invisible barrier protectors detect motion within a specific area, using either microwave or infrared technology.

A buried line sensor is, in essence, a chain link fence disturbance sensor, buried in the ground. A buried line sensor reacts to vibrations or pressure in a certain area.

An electric field sensor is composed of multiple wires. One has a current running throughout and the other acts as a sensing mechanism. When something enters the electromagnetic field that is in the wire, the energy in the wire is disturbed and activates an alarm.

CCTV System

Closed circuit television systems can be implemented to provide further protection to national security and other DoD assets. CCTV systems have a camera that captures a visual image, converts it to a video signal and transmits it to a remote location. At the remote location the image can be received, displayed, recorded, and printed.

CCTV is an excellent means for deterring and detecting loss, theft, or misuse of government property. CCTVs are used in a variety of facilities on installations and activities, including commissaries and exchanges. With CCTV, security personnel are able to monitor multiple areas simultaneously, thereby saving manpower.

CCTV is a reliable and a cost effective tool. It plays a very important role in our physical security mission.

Access Control System

Access control is a process for ensuring that only authorized personnel are allowed into a designated area. Access controls are implemented to prevent unauthorized personnel from entering designated areas. Access control is one of the inner layers in the overall security-in-depth approach. We learned earlier that physical security is like an onion; it has many layers until you get to the middle, the asset to be protected. The type of access control is determined during the risk management process.

There are different types of access control systems, from very simplistic manual systems, to more costly automated electronic systems.

One example of a manual system is the non-electronic cipher access control device. This stand-alone system only requires the user to know a 3 or 4 digit number in order to gain access.

An example of a manual system that uses automated electronics is the common access card (CAC). The CAC is the size of a credit card, and serves as the standard ID card for DoD. The CAC allows users to authenticate signatures and encrypt e-mails, securely log onto computer systems, and is also used as an access control device into designated areas. When used as a primary access control, security personnel must verify the CAC against the person entering the area.

Technology has provided many options in electronic automated access control systems. An example of a basic automated system is the electronic cipher. The motor in the electronic cipher is controlled by an electrical impulse which may be triggered in the following ways: by electronic card reader, proximity reader, keypad, or wireless remote control sensor. The electronic door lock is configured to start the motor-driven actuator once it has received the correct electronic input. More complex systems use biometrics. A biometric system uses individually unique human characteristics, such as fingerprints, hand geometry, handwriting, iris scan, and voice recognition. Biometric systems are employed to protect particularly sensitive DoD assets.

Screening Equipment

At DoD installations and facilities, you may encounter guard force personnel using x-ray machines, similar to those seen at airports, scanning hand carried baggage coming into a facility. Additional measures, including portable hand held metal detectors, permanently installed metal detectors, and other specialized equipment may also be used before personnel are granted access to certain areas.

Certain facilities have always utilized these types of equipment. However, since the terrorist attacks on the Murrah Federal Building in Oklahoma City in April 1995 and on the World Trade Centers on 9/11, more facilities have implemented these types of measures in an effort to protect national security and other DoD assets.

Two-way Radio

With any physical security system, communication is key. Two-way radios typically serve as the primary means of communication between response forces and their respective control centers, as well as communication between response force members. While two-way radios are a great tool, there must be backup communications systems available in the event of a catastrophic radio failure. A good Plan B is always necessary!

Facility Access Control

Facility access control procedures include identification systems, methods of control, and entry and exit inspections, which include search procedures for packages, vehicles, and

personal property. Controlling who and what enters a DoD installation or facility is of the utmost importance in our physical security mission.

Let's take a closer look at each facility access control procedure to learn more.

Identification Systems

Will the real John Jones please step forward? Are you who you say you are? Identification methods are one way of making sure you are who you say you are. This is yet another physical security countermeasure to protect national security and other DoD assets. There are a number of different identification systems being used for access to various areas on an installation or facility.

Homeland Security Presidential Directive (HSPD) 12, mandates common criteria for access control. Within DoD, the Common Access Card (CAC) is used to fulfill this requirement.

Some facilities, depending on the sensitivity of the area, may still require additional identification methods for entry. Various types of access control methods may be employed to include personal recognition, automated entry control systems, exchange badge systems, and security personnel conducting physical inspections of identification credentials.

Methods of Control

Does that person belong here? You may see a stranger who does not have the same badge as you, and you may wonder what they are doing in a secure area. It is always a good idea to be aware of your surroundings and the people in your secure area.

There are methods of control to assist with facility access. Escorts are used when rules require visitors to be under escort while inside an installation or facility. Access control rosters provide the names of those who are permitted access to a facility. Badging systems are also used to identify visitors, and in some cases, the two-person concept may be implemented, which requires two people to be present at all times while in a defined area. You should be able to validate whether an individual requires access to an installation or area, even if it is not their permanent assignment.

Entry and Exit Inspections

If you have entered a government facility recently, you have more than likely been through the inspection process. You may have had your vehicle searched, either randomly or during a high alert time. You may have had to place your belongings on an x-ray machine or passed through a metal detector to ensure you were not bringing unauthorized items into an area.

Installation and facility authorities determine criteria for conducting inspections of individuals, material in their possession, and vehicles, either randomly or each time an

individual or vehicle, enters or leaves a controlled area. Entry inspections include screening for illegal and prohibited articles such as recording devices, cell phones, and cameras.

Exit inspections may focus more on unauthorized removal of government assets, including classified information. This aspect of physical security is important because it serves not only as a great deterrent, but it also has value as a means to detect contraband.

Lock and Key Systems

We can never have too many layers protecting national security and other DoD assets. Guards may be employed to provide a level of security for certain areas, and we use security containers to safeguard classified information and other sensitive assets. Lock and key systems are used for protecting these assets.

Let’s take a look at the locks that are approved for DoD use and how we account for those locks.

Types of Locks

Within the DoD, there are two primary types of locks that you will see being used. These are combination and key-operated locks.

There are three types of approved combination locks used for the safeguarding of classified information. The first type is a built-in electromechanical lock used to secure classified material in security containers, vaults and other secure rooms. These locks meet the FF-L-2740 series federal specification which includes the Kaba Mas X-07, X-08, X-09, X-10, CDX-07, CDX-08, CDX-09 and CDX-10 locks as well as the Sargent and Greenleaf (S&G) 2740, 2740B, and 2890 Pedestrian Door Locks. The second type is the older style mechanical lock, the S&G 2937, which met prior standards and in some cases may still be used for classified storage. The third type is the combination padlock, S&G 8077/AD, which is approved for storage of Secret or Confidential bulk or temporary indoor storage. This lock meets the FF-P-110 series lock specification.

There are three types of key-operated locks used for other purposes. These are high and low security padlocks and mortise locks. High security key-operated padlocks include the S&G 833C and the S&G 951 and are approved for high security protection. Low security padlocks, sometimes referred to as secondary locks, are used for administrative control, on gates barring access to production facilities, for securing weapons racks contained within secured areas, and where secondary locks are specified. These locks provide only minimal resistance to forced or surreptitious entry and must not be used to secure classified material. Mortise locks, which include deadbolt and cylindrical locks, are typically found in general office areas and are also

considered low security locking devices. Cylindrical locks are the most common type of mortise door lock in use today.

The environment and type of asset to be protected will usually dictate what type of locking device is selected for use. Consult DoD regulations for specific lock and key requirements or refer to the Lock and Key Systems eLearning course offered by CDSE.

Key Control

Having a process in place to account for all locks and keys is essential. Key access and control measures can either be complex or simple, depending upon the program or regulatory requirements. At a minimum, lock and key control procedures should include a key register to list keys, document their issuance, return, and/or disposition. Another control measure would be to have a list of personnel who have authorized access to keys and key records. When keys are not being controlled and something goes missing, the corrective measures can be very costly, time consuming, and detrimental to the ability to protect DoD assets.

Storage Areas and Containers

You have learned about the many different layers of security it takes to maintain the physical security of a facility. Now we are going to discuss methods of storage, specifically, storage areas and security containers. Let's take a closer look at storage areas and security containers to learn more.

Storage Areas

There are several different methods used to secure large volumes of classified information. These include secure rooms, vaults, and sensitive compartmented information facilities (SCIFs).

Secure rooms are areas designated and authorized for the open storage of classified information. These facilities are usually built to commercial construction standards, and do not afford the extra security inherent with a "vault."

Vaults are constructed to meet strict forcible entry standards. Characteristics that set vaults apart from secure rooms include reinforced concrete on all walls, ceilings, and floors, plus a hardened steel door. When an area such as a secure room or a vault is approved for open storage, these areas must be constructed in accordance with DoD standards. Other requirements, such as alarms or guard checks, may be required. You should consult your component or agency authority for additional guidance.

The intelligence community uses a type of storage facility known as a SCIF for the storage of their sensitive compartmented information (SCI). SCI is derived from intelligence sources, methods, or analytical processes authorized by the Director of National Intelligence. When building a SCIF, there are strict standards that must be

adhered to. These standards address issues such as floors, ceilings, walls, locks, windows, and other openings. For additional information on SCIF construction, refer to the Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, IC Tech Spec for Intelligence Community Directive (ICD), and Intelligence Community Standard (ICS) 705..

Security Containers

General Services Administration (GSA) is the authority to approve security containers used to store classified information. Security containers approved for storage of classified information are tested and certified by GSA to ensure that a minimum level of protection against specified methods of unauthorized entry is provided. These containers must be equipped with locking devices that meet GSA standards. These locking devices were discussed earlier in this lesson. Weapons or sensitive items such as funds, jewels, precious metals, or drugs may not be stored in the same security container used to safeguard classified information. Storage of these items with classified material could increase the risk of compromise to classified information in the security container.

Review Activities

Review Activity 1

Question 1 of 3. Which of these can be made of solid steel to make them more attack resistant?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Walls
- ○ Doors
- ○ Windows
- ○ Roofs

Question 2 of 3. Which of these house ventilation systems that should be secured with steel bars?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Walls
- ○ Doors
- ○ Windows
- ○ Roofs

Question 3 of 3. Which of these should be covered with a protective film to make them less dangerous in an attack?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Walls
- ○ Doors
- ○ Windows
- ○ Roofs

Review Activity 2

Which of the following locks are approved to secure classified information or material?

Select all that apply. Then check your answers in the Answer Key at the end of this Student Guide.

☐ Kaba Mas X-10

☐ S&G 8077/AD

☐ S&G 833 C

Review Activity 3

Question 1 of 3. True or False. Standby lighting is used when regular lighting is not available.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

○ True

○ False

Question 2 of 3. True or False. Site lighting is used to enable guard force personnel to observe activities inside or outside the installation.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

○ True

○ False

Question 3 of 3. True or False. Movable lighting is used when supplemental lighting is needed such as at construction sites.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

○ True

○ False

Lesson 5: Physical Security Planning and Implementation

Introduction

Objective

In this lesson, you will learn about physical security planning, antiterrorism, and force protection, as well as the tools used to accomplish these critical functions.

Here are the lesson objectives:

- Identify the purpose of physical security planning and its tools
- Define antiterrorism and force protection and their tools

Physical Security Planning

Overview

Planning for the security defense of an installation or activity must be constant, practical, flexible to the mission, and responsive to the needs of the commander or director. Only through adequate planning can we provide an effective counter response to security threats.

Physical Security Plans

Physical security plans are comprehensive written plans providing for appropriate and economical use of personnel and equipment to prevent or minimize criminal or disruptive activities. It is essential that each installation, unit, or activity develop, implement, and maintain a physical security plan.

At a minimum, the plan should include special and general guard orders, access and material control, protective barrier and lighting systems, locks, and intrusion detection systems.

Physical security plans have the potential to be designated For Official Use Only (FOUO) or may even be classified, and must be protected accordingly.

SOPs and Post Orders

Standard operating procedures (SOPs) and Post Orders establish duties and responsibilities. This ensures that everyone involved knows the procedures so that duties are carried out consistently and uniformly. Using SOPs and Post Orders will assist in maintaining operational order during both normal and stressful situations.

SOPs are supplemental guidance for implementing specific components of your physical security program. SOPs are typically established to cover events such as fire, explosion, civil disturbance, major accidents, hostage situations, sabotage, bomb threats, terrorism attacks, and natural disasters. SOPs are also implemented to establish operational and administrative physical security procedures such as badging, escorts, and key control.

Post orders typically establish duties, roles, and responsibilities at individual assignments, checkpoints, gates, and guard posts.

Inspections

As a security professional, you may be a participant in a physical security inspection, either conducting an inspection, or being inspected. Inspections can ensure compliance with the physical security plan, verify policy compliance, promote cost effective security, serve as an opportunity for security education, establish and/or enhance good working relationships, identify existing or potential program weaknesses, and promote quality performance of security functions. As you can see, inspections serve many purposes. The results may be formally documented with observations, findings, and recommendations, or with informal discussions.

There are two types of inspections: compliance inspections and self-inspections.

Compliance Inspections

The compliance inspection focuses on ensuring regulatory requirements are being met, usually by someone who may be in your immediate chain of command or higher headquarters. Assist visits, command inspections, and Inspector General (IG) inspections are all examples of compliance inspections.

Self-inspections

A self-inspection is a review conducted by members of your own organization, usually with the aid of a checklist. Self-inspections may serve to aid internal control, prepare for compliance inspections, and ensure your physical security program is implemented in a cost effective manner.

Antiterrorism/Force Protection

Overview

Our nation has always been aware of potential terrorist threats. However, incidents such as the attack on the Murrah Federal Building in Oklahoma City, in April 1995 and the 9/11 terrorist attack, as well as various attacks around the world, have proven to us that there is a need for increased awareness of the probability that another terrorist attack will occur.

Let's take a look at terrorist threat levels, antiterrorism physical security measures, and Force Protection conditions (FPCONs) along with the responsibilities that our DoD installations and facilities have to protect our national security and other DoD assets.

Antiterrorism

Antiterrorism is defined as those defensive measures used to reduce the vulnerability of individuals and property to terrorist attacks, to include limited response and containment. Antiterrorism physical security measures integrate facilities, equipment, trained personnel, and procedures into a comprehensive effort designed to provide maximum protection to personnel and other DoD assets.

Well-designed physical security measures include: detection, deterrence, delay, denial, and notification. These efforts are accomplished through the development of an antiterrorism plan, outlining who will do what, where, when, and how.

This overview is intended to familiarize you with the basic terminology used in the DoD Antiterrorism Officer (ATO) Guide.

History has proven we must always be vigilant.

Terrorist Threat Levels

Terrorist threat levels are something many of us are aware of at this time in history. Terrorists are not just an ocean away any longer. Terrorist threat levels should not be confused with Force Protection Conditions, also known as FPCONs. Threat levels are provided to senior leaders in order to assist in determining the appropriate FPCON level.

DoD uses a set of standardized terms to quantify terrorist threat levels. Threat levels are identified as Low, Moderate, Significant, and High.

Low signifies no terrorist group is detected or the terrorist group is non-threatening.

Moderate signifies terrorists are present but there are no indications of anti-U.S. activity. The Operating Environment favors the Host Nation or the U.S.

Significant signifies anti-U.S. terrorists are present and they attack personnel as their preferred method of operation, or a group uses large casualty-producing attacks as their preferred method, but has limited operational activity. The Operating Environment is neutral.

High signifies anti-U.S. terrorists are operationally active and use large casualty-producing attacks as their preferred method of operation. There is a substantial DoD presence, and the Operating Environment favors the terrorist.

As a security professional, it is important to understand the relationship between physical security and terrorist threat levels.

FPCONs

Force Protection is defined as actions taken to prevent or mitigate hostile actions against DoD personnel, including family members, resources, facilities, and critical information.

Force Protection is implemented by establishing Force Protection Conditions, known as FPCONs. FPCONs are a DoD-approved system that standardizes the Department's identification and recommended preventive actions and responses to terrorist threats to U.S. assets.

There are five FPCONs for DoD. They are NORMAL, ALPHA, BRAVO, CHARLIE, and DELTA. For more information about the DoD Force Protection Condition System, refer to the DoD ATO Guide, which is marked For Official Use Only (FOUO).

FPCON Responsibilities

Commanders will fully implement the FPCON measures according to policy and remind their personnel to be alert for suspicious activities, such as the presence of unfamiliar personnel and vehicles, suspicious parcels, and possible surveillance attempts, and to report those activities in accordance with DoDI 2000.26, Suspicious Activity Reporting. Commanders also educate their personnel on the insider threat to DoD elements and personnel in accordance with the November 21, 2012 Presidential Memorandum and with DoDD 5205.16, The DoD Insider Threat Program. Finally, commanders comply with and integrate DoD physical security and installation access control policies into their FPCON plans.

The FPCON system allows commanders to be flexible and adaptable in developing and implementing antiterrorism measures that are more stringent than those mandated by higher authorities whenever FPCONS are invoked. Commanders may augment their FPCON by adding measures from higher FPCON standards as they deem necessary.

Review Activities

Review Activity 1

Question 1 of 3. At a minimum _________ should include special and general guard orders, access and material control, protective barriers, lighting systems, locks, and Intrusion Detection Systems (IDS).

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Standard Operating Procedures
- ○ Physical Security Plans
- ○ Post Orders

Question 2 of 3. ________ establish duties, roles, and responsibilities at individual assignments, checkpoints, gates, and guard posts.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Standard Operating Procedures
- ○ Physical Security Plans
- ○ Post Orders

Question 3 of 3. ___________provide supplemental guidance for physical security programs and establish procedures for emergency events as well as operational and administrative procedures.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Standard Operating Procedures
- ○ Physical Security Plans
- ○ Post Orders

Review Activity 2

Question 1 of 3. True or False. Commanders may only implement measures according to the FPCON level in force at the time.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ True
- ○ False

Question 2 of 3. True or False. Commanders must comply with and integrate DoD physical security and installation access control policies into their FPCON plans.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ True
- ○ False

Question 3 of 3. True or False. Commanders educate their personnel on the insider threat to DoD elements and personnel.

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ True
- ○ False

Lesson 6: Course Conclusion

Conclusion

Summary

In this course, you learned about how we secure our military installations and DoD facilities. You learned about the roles people fulfill in physical security, the method used to determine physical security countermeasures, the various types of countermeasures the DoD uses, and the tools it uses in physical security planning and implementation.

Objectives

Congratulations! You have completed the *Introduction to Physical Security* course.

You should now be able to perform the listed activities.

- Identify the terms, concepts, and policies associated with physical security
- Identify and define the roles and responsibilities of personnel in the physical security program
- Identify physical security countermeasures and their uses in the protection of DoD assets
- Describe physical security planning, antiterrorism, and force protection and their tools

To receive course credit, you must take the *Introduction to Physical Security* examination. If you accessed the course through the Security Training, Education, and Professionalization Portal (STEPP), please use that system to register for the online exam.

Appendix A: Answer Key

Lesson 2 Review Activities

Review Activity 1

Question 1 of 3. The two primary purposes of physical security are protection and _______________?

- ○ Security-in-depth
- ⦿ Prevention (correct answer)
- ○ Point security
- ○ Area security

Feedback*: The two primary purposes of physical security are protection and prevention.*

Question 2 of 3. A guard checking IDs at the gate of an installation is a good example of what type of security?

- ○ Security-in-depth
- ○ Prevention
- ⦿ Point security (correct answer)
- ○ Area security

Feedback: *A guard checking IDs is a good example of point security.*

Question 3 of 3. ___________ is the layering of physical security countermeasures such as fencing, guards, cameras, lighting, and locks.

- ⦿ Security-in-depth (correct answer)
- ○ Prevention
- ○ Point security
- ○ Area security

Feedback: *Security-in-depth is the layering of physical security countermeasures such as fencing, guards, cameras, lighting, and locks.*

Review Activity 2

Before you can conduct a risk analysis based on the impact and likelihood of an unwanted event happening, what steps in the risk management process must you take first?

- ☑ Identify assets (correct answer)
- ☑ Identify threats (correct answer)
- ☐ Determine countermeasure options
- ☑ Identify vulnerabilities (correct answer)
- ☐ Make risk management decisions

Feedback: *You must identify assets, threats and vulnerabilities before you can conduct a risk analysis based on the impact and likelihood of an unwanted event happening.*

Review Activity 3

Question 1 of 3. Which policy guidance would you consult to find the minimum standards for the physical protection of DoD assets?

- ⦿ DoD 5200.08-R, Physical Security Program (correct answer)
- ○ DoDI 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)
- ○ DoDM 5200.01, Volumes 1-4 DoD Information Security Program

Feedback: *You should consult DoD 5200.08-R, Physical Security Program, to find the minimum standards for the physical protection of DoD assets.*

Question 2 of 3. Which policy should you consult to find the physical security requirements of protecting classified information?

- ○ DoD 5200.08-R, Physical Security Program
- ○ DoDI 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)
- ⦿ DoDM 5200.01, Volumes 1-4 DoD Information Security Program (correct answer)

Feedback: *You should consult DoDM 5200.01, Volumes 1-4, DoD Information Security Program, to find the physical security requirements for protecting classified information.*

Question 3 of 3. Which policy authorizes commanders to issue regulations for the protection or security of property and places under their command?

- ○ DoD 5200.08-R, Physical Security Program
- ◉ DoDI 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB) (correct answer)
- ○ DoDM 5200.01, Volumes 1-4 DoD Information Security Program

Feedback: *DoDI 5200.08, Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB), authorizes commanders to issue regulations for the protection or security of property and places under their command.*

Lesson 3 Review Activities

Review Activity 1

Question 1 of 3. Who is charged with management, implementation, and direction of all physical security programs?

- ○ Law Enforcement
- ○ Antiterrorism Officer
- ○ OPSEC Officer
- ○ CI Support
- ◉ Physical Security Officer (correct answer)

Feedback: *The physical security officer is charged with management, implementation, and direction of all physical security programs.*

Question 2 of 3. Who is responsible for providing valuable information on the capabilities, intentions, and threats of adversaries?

- ○ Law Enforcement
- ○ Antiterrorism Officer
- ○ OPSEC Officer
- ◉ CI Support (correct answer)
- ○ Physical Security Officer

Feedback: *CI support is responsible for providing valuable information on the capabilities, intentions, and threats of adversaries.*

Question 3 of 3. Who is responsible for developing countermeasures against potential threats to national security and other DoD assets?

- ○ Law Enforcement
- ○ Antiterrorism Officer
- ⦿ OPSEC Officer (correct answer)
- ○ CI Support
- ○ Physical Security Officer

Feedback: *The OPSEC officer analyzes threats to assets and their vulnerabilities.*

Review Activity 2

Which of the following individuals should be included in a Threat Working Group?

- ☑ Antiterrorism Officer (correct answer)
- ☑ Counterintelligence (CI) representative (correct answer)
- ☑ Law enforcement representative (correct answer)
- ☑ Operations security officer (correct answer)
- ☑ Information operations representative (correct answer)
- ☑ Chemical, biological, radiological, nuclear and high yield explosive representative (correct answer)

Feedback: *All of these individuals should be included in a Threat Working Group (TWG). In addition, commanders of larger installations may choose to include more individuals in their TWG.*

Lesson 4 Review Activities

Review Activity 1

Question 1 of 3. Which of these can be made of solid steel to make them more attack resistant?

- ○ Walls
- ⦿ Doors (correct answer)
- ○ Windows
- ○ Roofs

Feedback: *Doors are a weak spot on a building and can be made of solid steel to make them more attack-resistant.*

Question 2 of 3. Which of these house ventilation systems that should be secured with steel bars?

- ○ Walls
- ○ Doors
- ○ Windows
- ⦿ Roofs (correct answer)

Feedback: *Roofs house air conditioning units and ventilation systems that should be secured with steel bars.*

Question 3 of 3. Which of these should be covered with a protective film to make them less dangerous in an attack?

- ○ Walls
- ○ Doors
- ⦿ Windows (correct answer)
- ○ Roofs

Feedback: *Windows should be covered with a protective film to make them shatter-proof.*

Review Activity 2

Which of the following locks are approved to secure classified information or material?

- ☑ Kaba Mas X-10 (correct answer)
- ☑ S&G 8077/AD (correct answer)
- ☐ S&G 833 C

Feedback: *The Kaba Mas X-10 is one of several locks that meet FF-L-2740 series lock specification which are approved for securing classified information. Sargent and Greenleaf (S&G) 8077/AD can be used for storage of Secret or Confidential bulk or temporary indoor storage.*

Review Activity 3

Question 1 of 3. True or False. Standby lighting is used when regular lighting is not available.

- ○ True
- ⦿ False (correct answer)

Feedback: *Emergency lighting is used when regular lighting is not available. Standby lighting is used when additional lighting is necessary.*

Question 2 of 3. True or False. Site lighting is used to enable guard force personnel to observe activities inside or outside the installation.

- ⦿ True (correct answer)
- ○ False

Feedback: *Site lighting is used to enable guard force personnel to observe activities inside or outside the installation.*

Question 3 of 3. True or False. Movable lighting is used when supplemental lighting is needed such as at construction sites.

- ⦿ True (correct answer)
- ○ False

Feedback: *Movable lighting is used when supplemental lighting is needed such as at construction sites.*

Lesson 5 Review Activities

Review Activity 1

Question 1 of 3. At a minimum _________ should include special and general guard orders, access and material control, protective barriers, lighting systems, locks, and Intrusion Detection Systems (IDS).

- ○ Standard Operating Procedures
- ⦿ Physical Security Plans (correct answer)
- ○ Post Orders

Feedback: *At a minimum physical security plans should include special and general guard orders, access and material control, protective barriers, lighting systems, locks, and Intrusion Detection Systems (IDS).*

Question 2 of 3. ________ establish duties, roles, and responsibilities at individual assignments, checkpoints, gates, and guard posts.

- ○ Standard Operating Procedures
- ○ Physical Security Plans
- ⦿ Post Orders (correct answer)

Feedback: *Post orders establish duties, roles, and responsibilities at individual assignments, checkpoints, gates, and guard posts.*

Question 3 of 3. ___________provide supplemental guidance for physical security programs and establish procedures for emergency events as well as operational and administrative procedures.

- ⦿ Standard Operating Procedures (correct answer)
- ○ Physical Security Plans
- ○ Post Orders

Feedback: *SOPs provide supplemental guidance for physical security programs and establish procedures for emergency events as well as operational and administrative procedures.*

Review Activity 2

Question 1 of 3. True or False. Commanders may only implement measures according to the FPCON level in force at the time.

- ○ True
- ⦿ False (correct answer)

Feedback: *The FPCON system allows commanders to be flexible and adaptable in developing and implementing antiterrorism measures that are more stringent than those mandated by higher authorities whenever FPCONS are invoked.*

Question 2 of 3. True or False. Commanders must comply with and integrate DoD physical security and installation access control policies into their FPCON plans.

- ⦿ True (correct answer)
- ○ False

Feedback: *Commanders must comply with and integrate DoD physical security and installation access control policies into their FPCON plans.*

Question 3 of 3. True or False. Commanders educate their personnel on the insider threat to DoD elements and personnel.

- ⦿ True (correct answer)
- ○ False

Feedback: *Commanders educate their personnel on the insider threat to DoD elements and personnel in accordance with the November 21, 2012 Presidential Memorandum and with DoDD 5205.16, The DoD Insider Threat Program.*